та. —2012. — № 6 (1). — С. 127–133.

2. Марков Ал. А. Об алфавитном кодировании. I // Докл. АН СССР. — 1960. — Т. 132. № 3. — С. 521–523.

3. Марков Ал. А. Об алфавитном кодировании. II // Докл. АН СССР. — 1961. — Т. 139. № 3. — С. 560–561.

4. Марков Ал. А. Нерекуррентное кодирование // Проблемы кибернетики. — 1962. — Вып. 3. — С. 169–186.

5. Яблонский С. В. Введение в дискретную математику. — М.: Наука, 1986.

6. Марков Ал. А. Введение в теорию кодирования. — М.: Наука, 1982.

DOI: 10.20948/dms-2022-89

О РАЗБИЕНИЯХ НА СОВЕРШЕННЫЕ КОДЫ В МЕТРИКЕ ХЭММИНГА

Ф. И. Соловьева **(Новосибирск)**

В настоящей работе приводятся две новые конструкции разбиений на совершенные коды в метрике Хэмминга. Вопрос построения таких разбиений остается недостаточно изученным (см. [1]), хотя является важным, поскольку тесно связан с проблемой перечисления q-ичных совершенных кодов с минимальным расстоянием 3 в векторном пространстве над полем Галуа. Обе конструкции разбиений являются комбинаторными, что может представлять интерес с практической точки зрения. Приведенные в работе методы построения базируются на двух конструкциях q-ичных совершенных кодов, принадлежащих Моллару [2, 3]. Одна из предложенных конструкций разбиений является свитчинговой, вторая – каскадной, идеи свитчинговых методов построения совершенных кодов см. подробно в [1].

Векторное пространство размерности n над полем Галуа $GF(q)$ по отношению к метрике Хэмминга обозначим через F_q^n. Параметры (длина, мощность кода и минимальное расстояние) q-ичного кода, необязательно линейного, обозначаются $(n, K, d)_q$. Совершенный q-ичный код — это код, достигающий границы Хэмминга. Далее будут

рассмотрены только q-ичные, $q > 2$, совершенные коды с минимальным расстоянием три.

1. Свитчинговая конструкция. Эта свитчинговая конструкция основана на методе построения q-ичных совершенных кодов Моллара 1983 г., см. [2]. Рассмотрим произвольный вектор $u \in F_q^{(q-1)n_1n_2}$ в следующем лексикографическом порядке: $u = (u_{1,1,1}, u_{1,1,2}, \ldots, u_{q-1,n_1,n_2})$ и для него введем две проверки на четность вида

$$s_i = \sum_{h=1}^{q-1} \sum_{j=1}^{n_2} u_{h,i,j} \text{ и } s'_j = \sum_{h=1}^{q-1} h \cdot \sum_{i=1}^{n_1} u_{h,i,j}.$$

Определим обобщенные проверки на четность $\pi_1(u) \in F_q^{n_1}$ и $\pi_2(u) \in F_q^{n_2}$ следующим образом:

$$\pi_1(u) = (s_1, s_2, \ldots, s_{n_1}), \;\; \pi_2(u) = (s'_1, s'_2, \ldots, s'_{n_2}).$$

Рассмотрим два произвольных разбиения пространств $F_q^{n_1}$ и $F_q^{n_2}$ на q-ичные совершенные коды C_s и C'_t с параметрами $(n_1 = (q^{m_1} - 1)/(q-1), K_1 = q^{n_1-m_1}, 3)_q$ и $(n_2 = (q^{m_2}-1)/(q-1), K_2 = q^{n_2-m_2}, 3)_q$ соответственно, где $s = 1, 2, \ldots, q^{m_1}, \quad t = 1, 2, \ldots, q^{m_2}$. Существование таких разбиений см., например, в [4], где использован метод свитчингов так называемых простых компонент, с использованием латинских квадратов, нижняя оценка числа таких различных q-ичных совершенных кодов дважды экпоненциальна.

Пусть φ — произвольное отображение из пространства $F_q^{n_1}$ в пространство $F_q^{n_2}$. Справедлива следующая

Теорема 1. *Совокупность кодов*

$$C_{s,t} = \{(u, x+\pi_1(u), y+\pi_2(u)+\varphi(x)) : u \in F_q^{(q-1)n_1n_2},\, x \in C_s,\, y \in C'_t\},$$

где $s = 1, 2, \ldots, q^{m_1}, \quad t = 1, 2, \ldots, q^{m_2}$, *образует разбиение пространства* F_q^n *на* q*-ичные совершенные коды с параметрами*

$$(n = (q^{m_1+m_2} - 1)/(q-1), K = q^{n-(m_1+m_2)}, 3)_q.$$

2. Каскадная конструкция. Данная каскадная конструкция базируется на методе построения q-ичных совершенных кодов Моллара 1984 г., см. [3]. Используем представление этой конструкции q-ичных совершенных кодов, предложенное Романовым в [5].

Пусть $\{C_a,\ a \in F_q^r\}$ — произвольное разбиение пространства F_q^n на q-ичные совершенные коды с параметрами $(n = (q^m - 1)/(q - 1), K = q^{n-m}, 3)_q$. Пусть $\{D_a,\ a \in F_q^r\}$ — произвольное разбиение некоторого MDS кода в $F_q^{n'}$ с минимальным расстоянием 2 на коды с параметрами $(n' = q^m, q^{n-m+1}, 3)_q$. Заметим, что оба разбиения необязательно являются разбиениями на классы смежностей кодов и необязательно коды в разбиениях линейны. Согласно [3, 5], для любого $q \geq 2$ и любой подстановки τ векторов пространства F_q^m совокупность векторов

$$C^* = \bigcup_{a \in F_q^r} C_{\tau(a)} \times D_a$$

является q-ичным совершенным кодом с параметрами $(N = (q^{m+1} - 1)/(q - 1), K = q^{n-m-1}, 3)_q$.

Построим, используя описанную конструкцию, разбиение на q-ичные совершенные коды длины N. Пусть $L_i = (\tau_{i1}, \tau_{i2}, \ldots, \tau_{iq^m})$ — произвольный латинский квадрат порядка q^m, $\quad i = 0, 1, \ldots, q - 1$. Через e_0 обозначим вектор веса 1 длины n' с единицей в первой координатной позиции.

Теорема 2. *Совокупность кодов*

$$C^*_{i,j} = \bigcup_{a \in F_q^r} C_{\tau_{ij}(a)} \times (D_a + i \cdot e_0),$$

где $i = 0, 1, 2, \ldots, q - 1,\ j = 1, 2, \ldots, q^m$, *образует разбиение пространства* F_q^N *на* q*-ичные совершенные коды с параметрами* $(N = (q^{m+1} - 1)/(q - 1), K = q^{n-m-1}, 3)_q$.

Известно, см. [6], что число различных, а также неэквивалентных, q-ичных совершенных кодов дважды экспоненциально. Поскольку в обоих представленных выше конструкциях участвуют разбиения на q-ичные совершенные коды, то, используя в этих итеративных конструкциях дважды экспоненциальные разбиения из работы [4], получим нижние оценки числа различных (и, следовательно, неэквивалентных) разбиений в обоих случаях также дважды экспоненциальными.

Исследование выполнено за счет гранта Российского научного фонда № 22-21-00135, https://rscf.ru/en/project/22-21-00135.

Список литературы

1. Соловьева Ф. И. Обзор по совершенным кодам // Математические вопросы кибернетики. — 2013. — Вып. 18. — С. 5–34.

2. Mollard M. Une g*é*n*é*ralisation de la fonction parit*é*, application *à* la conscruction de codes parfaits. Report de Recherche N. 395, Laboratoire de Math*é*matiques Appliqu*é*es, Grenoble, France, 1983.

3. Mollard M. Une novelle famille de 3-codes parfaits sur GF(q) // Discrete Mathematics. — 1984. — V. 49. — P. 209–212.

4. Соловьева Ф. И., Лось А. В. О построении разбиений F_q^n на совершенные q-значные коды // Дискретный анализ и исследование операций. — 2009. — Т. 16. вып. 3. — С. 63–73.

5. Романов А. М. On non-full-rank perfect codes over finite fields // Designs, Codes and Cryptography. — 2019. — V. 87. — N 5. — P. 995–1003.

6. Heden O., Krotov D. S. On the Structure of Non-Full-Rank Perfect q-Ary Codes // Advances in Mathematics of Communications. A special issue ALCOMA'10. — 2011. — V. 5. — N 2. — P. 149–156.

DOI: 10.20948/dms-2022-90

О СУЩЕСТВОВАНИИ A-ПРИМИТИВНЫХ РАЗБИЕНИЙ

Ю. В. Таранников (Москва)

Пусть q — степень простого числа. Достаточно широко известна задача разбиения пространства $\mathbb{F}_q^n$ на линейные подпространства L_i:

$$\{L_i\}: \qquad \bigsqcup_i (L_i \setminus \{0\}) = \mathbb{F}_q^n \setminus \{0\},$$

где L_i — линейные подпространства, как правило, одинаковой размерности (но не обязательно). Задача это не такая простая, но интересная, с большим числом приложений и активно изучавшаяся. Исследователей интересовало в основном существование разбиений и их структура; количество разбиений, как правило, не оценивалось.

В отличие от упомянутой выше задачи, практически не изучалась задача о разбиении $\mathbb{F}_q^n$ на аффинные подпространства $E_i = L_i + b_i$, где L_i — линейное подпространство, $b_i \in \mathbb{F}_q^n$:

$$\{E_i\}: \qquad \bigsqcup_i E_i = \mathbb{F}_q^n;$$